Şəbəkə təhlükəsizliyi əməliyyat mərkəzinin arxitektur modeli

Babək Nəbiyev

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

babek@iit.ab.az

Xülasə- **Bu məqalədə, şəbəkənin daha səmərəli və təhlükəsiz idarə edilməsini təmin etmək üçün yeni şəbəkə təhlükəsizliyi əməliyyat mərkəzi arxitekturunun yaradılmışdır. Bunun üçün aparılan araşdırmalar göstərir ki, hal-hazırda mövcud olan yanaşmaların bir çox zəif cəhətləri vardır. Mövcud olan yanaşmaların əsas zəif cəhətlərindən biri insan faktorunun iş prosesinin operativliyinə mənfi təsir göstərməsidir. Təqdim olunan arxitektur, şəbəkənin səmərəli və təhlükəsiz idarə edilməsi üçün müəyyən qərarların qəbul edilməsində köməklik göstərən və gələcəkdə baş verə biləcək hadisələrin qarşısında adaptiv qərarvermə qabiliyyətinə malikdir.**

Açar sözlər- şəbəkə təhlükəsizliyi; monitorinq; əməliyyat mərkəzi; arxitektur modeli

I. GİRİŞ

Şəbəkə təhlükəsizliyinin əməliyyat mərkəzi dedikdə şəbəkə haqqında informasiyanın toplayan, analiz edən, nəticələr haqqında qərarlar qəbulu edən, məlumatların əlaqədar şəxslərə və ya sistemlərə yönləndirən, müasir tələbləri ödəyən, proqram və aparat komplekslərindən ibarət olan mürəkkəb bir arxitektur nəzərdə tutulur.

Korporativ şəbəkənin infrastrukturunun genişləndirilməsi, təhlükəsizlik və monitorinq sistemlərinin işinin təşkili, mərkəzin resurslarından səmərəli istifadə, əlaqə kanallarının istifadəçilər arasında optimal paylanması, elektron sənəd dövriyyəsi sisteminin və videokonfrans xidmətinin təşkili, beynəlxalq səviyyədə, eləcə də digər ölkələrdə fəaliyyət göstərən müvafiq elmi şəbəkə qurumları ilə inteqrasiya istiqamətində kompleks işlərin həyata keçirilməsi üçün informasiya təhlükəsizliyinin və səmərəliliyinin artırılması vacibdir.

Bu istiqamət üzrə beynəlxalq çağırışlarda deyilir ki, informasiya təhlükəsizliyi ilə məşğul olan mərkəzlər yalnız profilaktik tədbirlərlə kifayətlənməməli, yeni hadisələrin aşkarlanması və qarşısının alınması üçün özlərini inkişaf etdirməlidirlər [1].

Şəbəkənin daha səmərəli və təhlükəsiz idarə edilməsini təmin etmək üçün yeni intellektual sistemin arxitekturu sintez olunmuşdur. Təqdim olunan yanaşma bir çox funksiyaların yerinə yetirilməsini təmin edir ki, bu da şəbəkənin səmərəliliyinin, təhlükəsizliyinin artırılmasına köməklik edir. Həmçinin şəbəkənin vəziyyətinin real-zaman rejimində operatorlar tərəfindən daimi izlənməsi üçün xüsusi vizuallaşdırma ekranları da mövcuddur. Şəbəkə təhlükəsizliyi əməliyyat mərkəzi (ŞTƏM) şəbəkədə meydana çıxan təhdidlər haqqında vaxtında xəbərdarlıq edir və şəbəkə mühitində real zaman rejimində işləyir.

II. ƏLAQƏDAR İŞLƏR

ŞTƏM kimi şəbəkə təhlükəsizliyinin əməliyyat mərkəzi fəaliyyətini yerinə yetirən bir çox sistemlər və mərkəzlər vardır. Kiçik və böyük miqyaslı, bircinsli və ya hibrid şəbəkələrin təhlükəsizliyinin təmin olunması üçün kompleks yanaşmalar mövcuddur. Bu yanaşmalar kompleks və ya ayrı-ayrı həllər formasında bir çox şəbəkələrdə mövcuddur. Amma mövcud sistemlərin və ya mərkəzlərin bir çox hallarda rutin, təkrarlanan və ya böyük həcmdə informasiyanın emalı ilə bağlı problemlərinin olduğu məlumdur [2].

Bu sistemlərin və mərkəzlərin işinin tənzimlənməsi üçün bir çox standartlar, siyasətlər və məsləhət tipli qaydalar mövcuddur [3, 4]. Bu sistem və ya mərkəzlərə misal olaraq informasiya təhlükəsizliyi insidentlərinə reaksiya komandası (ing. Computer Security Incident Response Services, CSIRT), informasiya təhlükəsizliyi insidentlərinə reaksiya komandalarının forumu (ing. Forum of Incident Response and Security Teams, FIRST), informasiya təhlükəsizliyi idarəetmə sistemi (ing. Information Security Management System, ISMS), təhlükəsizlik əməliyyatları mərkəzlərini (ing. Security Operation Center, SOC) və s. göstərmək olar.

CSIRT informasiya təhlükəsizliyi insidentlərinə reaksiya komandasıdır [5]. Bu komanda təhlükəsizlik hadisələri haqqında informasiyanı alır, onu analiz edir və göndərən tərəfə cavab verir. CSIRT komandası sabit və ya ad-hoc ola bilər. İki tip CSIRT mövcuddur: daxili və xarici. Daxili CSIRT hər hansı bir təşkilatın tərkibində fəaliyyət göstərib korporativ təhlükəsizliyin dəstəklənməsi ilə məşğul olursa, xarici CSIRT kommersiya fəaliyyəti ilə məşğul olur. CSIRT informasiya təhlükəsizliyi üzrə müəyyən olan insidentlərin hamısı və ya bir neçəsi üzrə ixtisaslaşmış ola bilər. Bundan savayı tədris və KİV-də təbliğatla da məşğul ola bilərlər.

FIRST kompüter təhlükəsizliyi insidentlərinin həllində daha səmərəli qərarların qəbul edilməsi üçün insidentə cavab və təhlükəsizlik komandaları arasında əlaqələrin daha da asanlaşdırılması üçün nəzərdə tutulmuşdur [6]. FIRST-ün tərkibinə daxil olan komandalar toplusu insidentə və təhlükəsizliyə cavab verən geniş şəkilli ekspertiza təşkil edir. FIRST insidentə cavab və təhlükəsizlik komandaları arasındakı etibarlı qarşılıqlı əlaqəni təmin etmək üçün forum təşkil edir. Qarşılıqlı əlaqəyə kömək o zaman mümkündür ki, hər iki tərəfdən komandaların bazaları birləşdirilsin (birbaşa komandaları daxil etməklə) və ya FIRST-ün təhlükəsiz

DOI: 10.25045/NCInfoSec.2017.23

rejimdə bütün üzvlər arasında informasiyanın bölüşdürülməsi infrastrukturundan istifadə edilsin. Bərabərhüquqlu komandalar arasında məlumatı ötürmək bacarığının artırılması informasiya təhlükəsizliyi insidentlərinin - mənbəyindən, təyin olunduğu və keçdiyi yerdən asılı olmayaraq tez aradan qaldırılmasına imkan verir.

ISMS informasiya təhlükəsizliyi idarəetmə sistemidir və təşkilatın konfidensial məlumatlarının sistematik idarəolunması üçün özündə siyasətlər toplusunu və təhlükəsizlik prosedurlarını birləşdirir [7]. ISMS-in əsas məqsədi təhlükəsizliyə təsir edə biləcək hadisələrin qarşısının aktiv formada alınması, risklərin minimallaşdırılması və bunun əsasında təşkilatın fəaliyyətinin fasiləsizliyini təmin etməkdir. ISMS-in yaradılması üçün [3]-də göstərilən standartdan istifadə olunur.

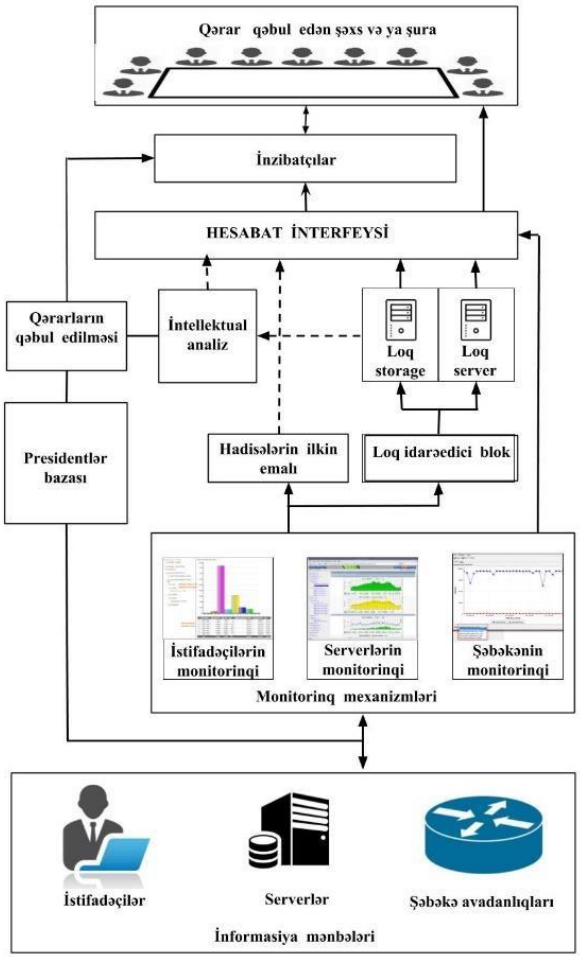
SOC təşkilati və texniki təhlükəsizlik məsələləri ilə məşğul olan mərkəzdir. [8]–də göstərildiyi kimi, bu mərkəzin əməliyyat qabiliyyəti isə aşağıdakı bloklar əsasında realizasiya olunur: verilənlərin generatoru olan sensorlar, verilənlərin saxlanılması üçün toplama bloku, ümumi formata uyğunlaşdırılmış verilənlər bazası, insidentlərin analizi, biliklər bazası, qərar və hesabat. Bütün bu bloklar kompleks formada təhlükəsizliyin təmin olunması mərkəzinin komponentlərini təşkil edir.

Bildiyimiz kimi böyük həcmdə informasiya generasiya edən şəbəkələr mövcuddur. Bu cür şəbəkələr həm yaxın məkanlarda, həm də başqa saat qurşağında yerləşən şəbəkələri özündə birləşdirir. Belə şəbəkələrin generasiya etdiyi informasiyalar yüzlərlə Tb-larla ölçülür. Böyük informasiya generasiya edən şəbəkələrin loq faylları və hadisələrin qeydiyyatı jurnalları özündə çox böyük həcmdə informasiya cəmləyir. Belə böyük informasiyaların həlli üçün Big Data texnologiyalarının tətbiqi labüddür. Həm də Big Data sayılan verilənlərin emalı üçün yüksək hesablama gücü tələb edilir. Buna görə də bu cür yanaşmalar cloud texnologiyalar bazasında realizasiya olunur. Bunlardan birinə misal olaraq arxitekturu və texnoloji aspektləri Cisco şirkəti tərəfindən təklif olunmuş Apache Metron proqram təminatını misal göstərmək olar [10]. Cloud bazasında realizasiya olunan texnologiyaların hamısında olduğu kimi, bu yanaşmada da əgər əlaqə kanallarında problem baş verərsə, avtonom rejimdə bu prosesləri realizasiya etmək mümkün olmayacaq.

III. ARXİTEKTUR MODELİ

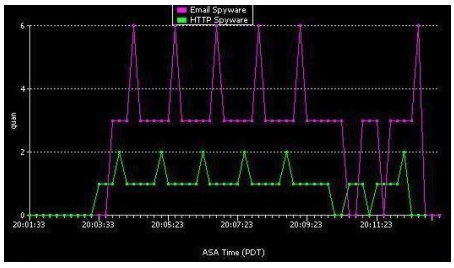
Şəbəkənin daha səmərəli və təhlükəsiz idarə edilməsini təmin etmək üçün yeni arxitektur yaradılmışdır. Təqdim olunan arxitektur şəbəkənin səmərəli və təhlükəsiz idarə edilməsi üçün müəyyən qərarların qəbul edilməsinə köməklik göstərir (Şəkil 1).

Bu arxitekturda hadisələrin aşkarlanması, təsnifatı və qərarvermə prosesi intellektual analiz metodları vasitəsilə həyata keçirilir. İntellektual analiz metodları şəbəkələrarası ekranlarda realizasiya olunmuşdur və bu baş verə biləcək hadisələrə operativ və birbaşa müdaxilə etmək üçün əlverişlidir. Şəbəkələrarası ekranın, trafikdə axan kontentin idarəolunması və təhdidlərin aşkarlanması funksiyaları da mövcuddur. Bu isə zərərli proqramlardan kompleks qorunma, genişləndirilmiş kontent filtirasiyası, e-məktubların inteqrasiya olunmuş təhlükəsizliyi kimi bilinən anti-spam texnologiyası, şəbəkənin profilinə uyğun sazlanması və s. funksiyaları özündə cəmləşdirilməsi deməkdir.



Şəkil 1. Şəbəkə təhlükəsizliyi əməliyyat mərkəzinin arxitekturunun sintezi

Məsələn, bədniyyətli tərəfindən göndərilən e-mail və ya paketlərin real zaman anında müəyyən olunması haqqında hesabat şəkil 2-də göstərilmişdir.



Şəkil 2. Zərərli e-mail və ya paketlərin real zaman anında müəyyən olunması haqqında hesabat

Hazırda mövcud olan şəbəkə təhlükəsizliyi mərkəzlərində təhlükəsizlik hadisələri haqqında qərarların qəbul edilməsi tamamilə insan faktorundan asılıdır və bu fəaliyyəti həyata keçirən insanlardan böyük əmək, təcrübə və bilik tələb olunur. İnformasiya təhlükəsizliyinin emalı üzrə qəbul edilmiş qərarlar bir çox halda əvvəllər qazanılmış təcrübəyə, qəbul edilmiş qərarlara əsaslanır və yeri gəldikdə onların yeni

situasiya üçün adaptasiya edilməsinə ehtiyac duyulur. Presedentlər əsasında mövcud vəziyyətə uyğun hazır həllin verilməsini təmin edən aparat “presedentlər nəzəriyyəsi”dir (ing. Case-Based Reasoning, CBR) [9].

Əvvəlcədən aşkarlanmış və müvafiq tədbir görülmüş insidentlərin həlli yolları presedentlər bazasında yerləşdirilir. Yəni, hazır həllər yaddaşı kimi mərkəzdə presedentlər bazası yerləşdirilib. Yeni problem baş verdikdə onun əlamətləri qeydiyyatdan keçirilir və bu da presedentlər bazasından problemlərin axtarılmasını təmin edir. Aydındır ki, funksiyaların oxşarlıq səviyyəsi nə qədər yaxındırsa, presedentlərin axtarış effektivliyi də bir o qədər yüksək olar [2].

Qərarları qəbul edən şəxs və ya qrup presedentlər bazasında uyğun presedent tapmadığı halda qərar əvvəlcədən müəyyən olunmuş ekspertlər tərəfindən qəbul olunur.

Qərarlara dəstək sistemi hər iki halda – uyğun presedent tapıldığı və ya tapılmadığı halda qəbul olunmuş qərarı təhlükəni zərərsizləşdirmək üçün proseslərə və eyni zamanda hesabat formasında aidiyyatı şəxslərə ötürür. Yeni insidentlər və onların həlləri dəqiqləşdirildikdən sonra bu həllər yekun qərar vermək hüququ olan aidiyyatı şəxslər tərəfindən hazır həllər bazasına ötürülür.

IV. ŞƏBƏKƏNİN MONİTORİNQİ

ŞTƏM-in işinin təmin olunması üçün sistem fəaliyyət göstərir. Bu sistem də həmin mərkəzin tərkib hissəsidir. Eyni zamanda mərkəzin tərkib hissəsi olan sistemin fəaliyyəti üçün proqram təminatları yaradılmışdır. Yaradılan proqram təminatları şəbəkədə meydana çıxan təhdidlər haqqında vaxtında xəbərdarlıq edir. Sistem şəbəkə mühitində real zaman rejimində işləyir. Bu sistemdə şəbəkənin vəziyyətinin real-zaman rejimində daimi operatorlar tərəfindən izlənməsi üçün xüsusi vizuallaşdırma ekranları da mövcuddur.

Bu sistemin informasiya mənbəyi şəbəkənin hər bir səviyyəsi üzrə informasiya axınlarıdır. Şəbəkədə baş verən proseslərin monitorinqini aparmaq üçün üç informasiya mənbəyi seçilmişdir:

1. şəbəkə avadanlıqları;
2. serverlər;
3. istifadəçilər.

Şəbəkə avadanlıqlarının monitorinqi dedikdə, şəbəkədə fəaliyyət göstərən bütün şəbəkə avadanlıqlarının əməli yaddaşının, temperaturunun, yüklənməsinin, əlaqə kanallarının vəziyyətinin, axan trafikinin sürətinin monitorinqi nəzərdə tutulur (şəkil 3).

Şəkil 3. Şəbəkə avadanlıqlarının monitorinqinin hesabatı

Bundan savayı şəbəkədə fəaliyyət göstərən bütün şəbəkə avadanlıqlarının bir-biri ilə birləşmə topologiyası və ayrılıqda onlara birləşmiş əlaqə kanallarının topologiyasını formalaşdıran və vizualizasiya edən vasitələrdən də istifadə olunur.

Yuxarıda nəzərdə tutulan tədbirlər şəbəkə monitorinqi funksiyasını yerinə yetirir və informasiya təhlükəsizliyi əməliyyat mərkəzinin bir hissəsidir.

Monitorinqin digər mərhələlərindən biri serverlərin monitorinqidir. Bu serverlər müxtəlif xidmətlər üçün fəaliyyət göstərirlər. Bu xidmətlərin hamısının iş fəaliyyətinin təmin olunması üçün müxtəlif server avadanlıqlarından istifadə olunur. Bu server avadanlıqlar VMware ESXi, FreeBSD, Ubuntu, RedHat, CentOS, Windows, SUSE Linux və s. müxtəlif əməliyyat sistemləri üzərində çalışırlar. Bu əməliyyat sistemləri bir və ya bir neçə xidmət üçün fəaliyyət göstərir. Hər bir əməliyyat sisteminin üzərində ayrı-ayrılıqda monitorinq aparılması prosesi çoxlu sayda sazlama, insan resursu və zaman tələb etdiyi üçün server avadanlıqlarının birbaşa özlərinin vəziyyətlərinin monitorinq olunması və öyrənilməsi məqsədə uyğundur.

Ən son monitorinq mexanizmlərindən biri istifadəçilərin monitorinqidir. İstifadəçilərin monitorinqi sistemi şəbəkədə istifadəçi səviyyəsində texnologiyanın imkan verdiyi bütün informasiyanın qeydiyyatı və vizuallaşdırılması ilə məşğul olur və ən çox informasiya resursu tələb edir.

İstifadəçilərin identifikasiyası və məkanın müəyyən olunması üçün reyestr sistemi qurulmuşdur. Bu reyestr sistemi bütün şəbəkəni əhatə edir və onun xidmətlərindən istifadə etməyə imkan verir.

İstifadəçilərin siyahısı cədvəl şəklində VLAN-lara (ing. Virtual Local Area Network) qruplaşdırılıb və eyni zamanda istifadəçi axtarış sistemi vasitəsi ilə aşağıdakı meyarlara görə tapıla bilərlər:

- ad, soyad;
- VLAN (istiqamət, bina);
- İP ünvan;
- MAC ünvan;
- binanın mərtəbəsi, otağın nömrəsi, kompüterin nömrəsi;
- telefon nömrəsi;
- əlavə qeydlər (vəzifəsi və s.);

Hər üç monitorinq mexanizmi vasitəsilə toplanmış loqlar sonrakı analiz üçün loq serverə göndərilir. Bu proses avtomatlaşdırılıb və hər 24 saatdan bir baş verir. Loq fayllar hər VLAN üzrə və hər monitorinq mexanizmi üzrə ayrı-ayrılıqda zaman ştampı vurularaq saxlanılır. Bu loqlardan hər hansı eksperiment üçün istifadə etmək mümkündür. Buna misal olaraq, toplanan loq fayllar vasitəsilə elmmetriya hesabatı, ayrı-ayrı institutlar üçün İnternetdən istifadə hesabatları və s. hazırlanmasını göstərmək.

Bu verilənlərin elmi-analitik və təhdidlərin aşkarlanması nöqteyi-nəzərindən lazım gəldikdə emal oluna bilməsi üçün loq fayllar uzun müddət saxlanılır. Həmin loq fayllar müxtəlif analiz proqram vasitələri üçün əlverişlidir.

Misal üçün aşağıdakı hesabatlar generasiya oluna bilər:

1. Domen zonalar üzrə hesabat;

2. Trafikin veb-saytlar üzrə hesabatı;
3. Həftənin günləri üzrə hesabat;
4. Saatlar üzrə hesabat;
5. Veb-saytların profilinə görə trafikin paylanması;
6. IP ünvan üzrə hesabat;
7. IP qruplar üzrə hesabat;
8. Yaş həddinə görə hesabat;
9. AntiSpam sistemi üzrə hesabatlar.

Bu hesabatlar da bir neçə alt-hesabatlara bölünür:

1. Müraciətlərin həcmi
2. Müraciətlərin sayı

Müraciət dedikdə şəbəkədə baş verən hər bir sorğu nəzərdə tutulur. Bu anlayış IP ünvana, URL-ə, istifadəçilərə, kontentə və s. şamil edilə bilər.

Nəzərə alsaq ki, loqlama prosesi bütün şəbəkə və istifadəçilər üçün aparılır, bu sistemin necə həssas informasiya kütləsinə malik olduğu nəzərə çarpır. Buna görə də, loq faylların saxlanılması və idarə edilməsi üçün xüsusi olaraq loqların idarəetmə bloku yaradılmışdır. Loqların idarəetmə bloku özü-özlüyündə iki hissəyə bölünür:

- Loq server
- Loq storage

Loq server loqların qəbul olunması və çeşidlənməsi funksiyasını yerinə yetirir. Loq storage isə bu loq faylların saxlanılması üçün istifadə olunur.

Loq fayllar 24 saat ərzində generasiya olunduğu serverdə toplanır və günün axırında fayl formasında toplanıb loq servere göndərilir. Bu prosesin aparılması yaradılmış xüsusi proqram təminatı vasitəsilə realizasiya olunur.

Loq server isə öz növbəsində daxil olan loq faylı və ya faylları göndərilən serverə və loq tipinə uyğun olaraq seçir, lazımi qovluğa yerləşdirir. Loq fayllar özündə həssas informasiya daşıdığı üçün sistemə 24/7 nəzarət olunur və baş verən hadisələr haqqında sistem avtomatik olaraq inzibatçını məlumatlandırır. Bu sistemə və verilənlər bazasına giriş etibarlılığın və təhlükəsizliyin təmin olunması üçün xüsusi kripto açarlarla qorunur və bu açarlar müntəzəm olaraq yenilənir.

V. ARXİTEKTUR MODELİN TƏTBİQİ

Şəbəkə Təhlükəsizliyi Əməliyyat Mərkəzi hal-hazırda AzScienceNet şəbəkəsində eksprimental formada fəaliyyət göstərməkdədir.

AzScienceNet şəbəkəsində 20-yə yaxın xidmət fəaliyyət göstərir. Bunlara misal olaraq, AzCloud xidməti, hostinq xidməti, eduroam xidməti, elektron poçt xidməti, OwnCloud, distant təhsil xidməti, İP telefoniya xidməti, onlayn TV yayımı xidməti, operativ məlumatlandırma sistemi və s. xidmətləri göstərmək olar.

Bu mərkəzin istifadəçi monitorinqi sistemi AMEA Prezidentinin qərarı ilə təsdiq olunmuş “İstifadəçi siyasəti” əsasında fəaliyyət göstərir.

AzScienceNet şəbəkəsi 40 institut və təşkilat üzrə fəaliyyət göstərir və bunların hər biri bir VLAN-dır . Yəni AzScienceNet şəbəkəsində hər bir VLAN üzrə orta hesabla 170-ə yaxın istifadəçi vardır, bu isə ümumilikdə 6000-dən çox istifadəçi deməkdir.

NƏTİCƏ

Bu məqalədə şəbəkə təhlükəsizliyi mərkəzinin sintez arxitekturu təqdim olunmuşdur. Bu arxitekturda informasiya təhlükəsizliyi hadisələrinin aşkarlanması, qarşısının alınması haqqında düzgün qərarların qəbul olunması prosesi izah olunmuşdur. Belə mərkəzlərin fəaliyyəti və baş mərkəz altında koordinasiyası gələcəkdə baş verə biləcək hadisələrin qarşısının əvvəlcədən alınmasına kömək edə biləcək.

ƏDƏBİYYAT

[1]. T. Schmidt, R. Aeberhardt, S. Wenigmann, A. Rogg, "Cybersecurity services EY Financial Services Advisory", 2016, Ernst & Young Media p. 17.

[2]. Y.N. İmamverdiyev, B.R. Nəbiyev, “Şəbəkə təhlükəsizliyinin intellektual monitorinqi üçün konseptual model” Informasiya Cəmiyyəti Problemləri, 2017, №1, s. 81-89

[3]. AZS 494-2010 (ISO/IEC 27001-2005) İnformasiya Təhlükəsizliyi. Təhlükəsizlik metodları. İnformasiya təhlükəsizliyinin idarə edilməsi sistemləri. Tələblər. 2010.

[4]. M. Daniele, IP Version 6 Management Information Base for the Transmission Control Protocol, www.ietf.org/rfc/rfc2452.txt

[5]. Computer Security Incident Response Team, www.whatis.techtarget.com/definition/Computer-Security-Incident-Response-Team-CSIRT

[6]. Forum of Incident Response and Security Teams, www.first.org

[7]. İnformation security management system, www.whatis.techtarget.com/definition/information-security-management-system-ISMS

[8]. N. Miloslavskaya, “Security Operations Centers for Information Security Incident Management” IEEE 4th International Conference on Future Internet of Things and Cloud, 2016, pp. 25-36

[9]. Y.N. İmamverdiyev, B.R. Nəbiyev, “Presedentlər nəzəriyyəsi əsasında şəbəkə təhlükəsizliyinin monitorinqi üzrə qərarlarin qəbulu metodu” İnformasiya Texnologiyaları Problemləri, 2012, №2, s. 53-58

[10]. Apache Metron Overview, https://cwiki.apache.org/confluence/display/METRON/Metron+Wiki

ARCHITECTURE MODEL OF THE NETWORK SECURITY CENTER

Babak Nabiyev
Institute of Information Technology of ANAS, Baku, Azerbaijan
babek@iit.ab.az

Abstract – This article demonstrates the importance of creating a new network security operating center architecture to ensure a more efficient and secure network management. Research to do so shows that the approaches currently underway have many weaknesses. One of the main weaknesses of the approaches is that the human factor negatively affects the operational process. The proposed architecture is an adaptive decision-making approach to helping make certain decisions in order to effectively and securely manage the network and to handle future events.

Keywords – network security; monitoring; operating center; architecture model